KAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Ekonomi dan Manajemen
Vol.1, No.4 Desember 2023
e-ISSN: 3025-7859; p-ISSN: 3025-7972, Hal 173-181
DOI: https://doi.org/10.61722/jiem.v1i4.331

ANALISIS PERLINDUNGAN NASABAH BSI TERHADAP KEBOCORAN DATA DALAM MENGGUNAKAN DIGITAL BANKING

Dewi Fatmala Putri
Institut Agama Islam Negeri (IAIN) Kediri
Andriani
Institut Agama Islam Negeri (IAIN) Kediri
Widya Ratna Sari
Institut Agama Islam Negeri (IAIN) Kediri
Faricha Lita Nabbila
Institut Agama Islam Negeri (IAIN) Kediri

Alamat: Jl. SunanAmpel No. 07 Ngronggo Kota Kediri, Kediri, Jawa Timur 68137
Korespondensi penulis: dewifatmalap@gmail.com, andriani@iainkediri.ac.id, widyaratnasari99@gmail.com, farichalita@gmail.com

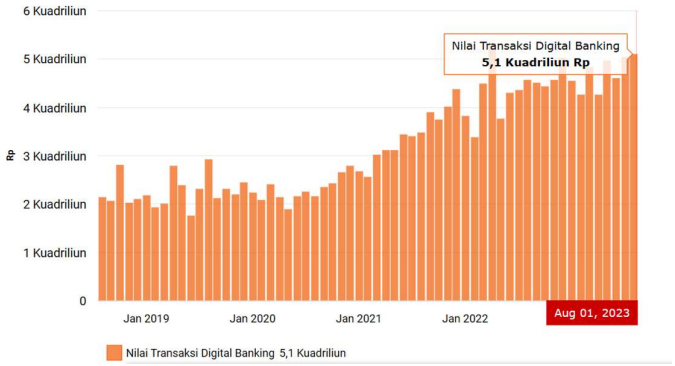
Abstrac
However, the increasing cyberattacks in the financial sector indicate that customer protection is crucial. Security risks such as phishing, malware, and service disruptions can harm customers and threaten trust in banking institutions. The analysis of BSI customer protection involves understanding security policies, responses to cyberattacks, and customer data protection policies. The research method used is qualitative descriptive, with data collection through literature, news, interviews, and direct observations. The discussion involves the analysis of BSI digital services, security risks, legal protection for customers, and security protocols applied by BSI. The research highlights the importance of enhancing resilience against cyberattacks and maintaining reliable information technology infrastructure. The literature review includes consumer protection, digital banking, and digital financial services. Consumer protection is regulated by Law Number 8 of 1999, while digital banking and digital financial services provide extensive efficiency and accessibility.
Keywords: *Customer Protection, Data Breaches, Digital Banking*

Abstrak
Meningkatnya serangan siber di sektor keuangan menunjukkan bahwa perlindungan nasabah menjadi krusial. Terdapat risiko keamanan seperti phishing, malware, dan gangguan layanan, yang dapat merugikan nasabah dan mengancam kepercayaan terhadap institusi perbankan. Analisis perlindungan nasabah BSI melibatkan pemahaman terhadap kebijakan keamanan, respons terhadap serangan siber, dan kebijakan perlindungan data nasabah. Metode penelitian yang digunakan adalah deskriptif kualitatif, dengan pengumpulan data melalui literatur, berita, wawancara, dan pengamatan langsung. Pembahasan melibatkan analisis layanan digital BSI, risiko keamanan, perlindungan hukum nasabah, dan protokol keamanan yang diterapkan oleh BSI. Hasil penelitian menyoroti pentingnya peningkatan ketangguhan terhadap serangan siber dan infrastruktur teknologi informasi yang handal. Kajian literatur mencakup perlindungan konsumen, digital banking, dan layanan keuangan digital. Perlindungan konsumen diatur oleh Undang-Undang Nomor 8 Tahun 1999, sementara digital banking dan layanan keuangan digital memberikan efisiensi dan aksesibilitas yang luas.
Kata Kunci: Perlindungan Nasabah, Kebocoran Data, Digital Banking

Received Oktober 30, 2023; Revised November 2, 2023; Desember 7, 2023
*Corresponding author, e-mail address

LATAR BELAKANG

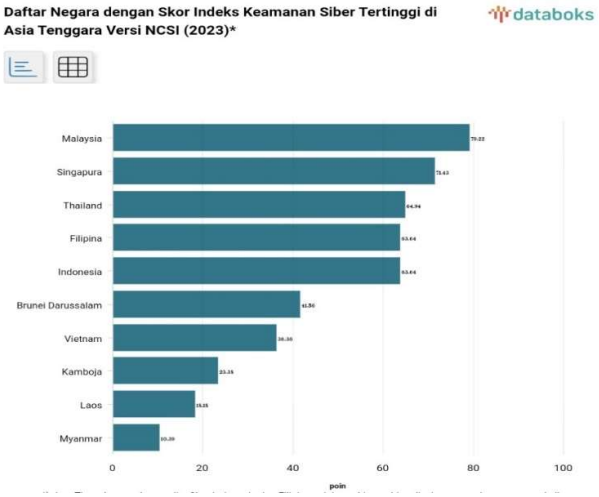
Dalam era ekonomi digital yang berkembang pesat, transformasi digital telah mengubah banyak aspek kehidupan, termasuk sektor perbankan. Digital banking menjadi salah satu inovasi utama yang memfasilitasi akses perbankan secara efisien melalui platform online. Digital banking mencakup berbagai layanan perbankan yang dapat diakses melalui perangkat elektronik, seperti komputer, smartphone, atau tablet. Era ekonomi digital didefinisikan oleh integrasi teknologi informasi dan komunikasi dalam semua aspek aktivitas ekonomi. Digital banking adalah layanan perbankan yang memungkinkan nasabah untuk melakukan transaksi keuangan melalui internet atau aplikasi mobile banking. Era ekonomi digital yang semakin berkembang telah memudahkan akses ke layanan perbankan ini.



Menurut laporan Nilai transaksi digital banking di Indonesia pada bulan Agustus 2023 mencapai Rp5,1 kuadriliun atau sekitar $350 miliar. Nilai ini meningkat sebesar 1,3% dibandingkan dengan bulan Juli 2023 dan tumbuh sebesar 11,9% dibandingkan dengan periode yang sama tahun sebelumnya . Transaksi digital banking mencakup transaksi internet banking, SMS/mobile banking, dan phone banking.

Hal tersebut menunjukan bahwa kebutuhan akan adanya digital banking terus meningkat. Hal ini mendorong adanya transformasi ini membawa kemudahan dan efisiensi, termasuk dalam akses dan pengelolaan keuangan. Di Indonesia, Bank Syariah Indonesia (BSI) sebagai salah satu lembaga keuangan terkemuka telah mengadopsi digital banking untuk meningkatkan layanan kepada nasabahnya. Bank Syariah Indonesia (BSI) sebagai lembaga keuangan berbasis syariah juga mengambil bagian dalam era ekonomi digital ini dengan menyediakan layanan digital banking yang sesuai dengan prinsip-prinsip syariah.

Perbankan digital telah menjadi semakin populer karena kenyamanan dan manfaat penghematan waktu. Perlindungan nasabah dalam menggunakan digital banking menjadi isu yang penting karena adanya ancaman keamanan seperti pencurian identitas, penipuan, gangguan pada transaksi, serangan malware yang dapat merusak sistem keamanan digital banking dan kebocoran data pribadi.(Rahmah, 2018) Oleh karena itu, analisis terhadap perlindungan nasabah Bank Syariah Indonesia (BSI) dalam menggunakan layanan digital banking digital menjadi suatu hal yang tidak hanya penting, tetapi juga krusial. Digitalisasi pada sektor keuangan meningkatkan probabilitas serangan siber hingga 86,70%. IMF (International Moneter Fund) memperkirakan total kerugian rata-rata tahunan yang dialami sektor jasa keuangan secara global yang disebabkan oleh serangan siber yaitu senilai USD100 miliar atau lebih dari Rp1.433 triliun.(Rizki, 2022) Indonesia sediri menduduki peringkat ke lima dalam keamanan dari siber di Asia Tenggara.



Berdasarkan laporan National Cyber Security Index (NCSI), Indonesia masuk lima besar negara dengan keamanan siber terbaik di kelompok Association of Southeast Asian Nations (ASEAN) pada 2023. Indonesia meraih penilaian sebesar 63,64 poin dari skor maksimal 100 poin. Sementara secara global, Indonesia menduduki peringkat ke-49 dari 176 negara yang diriset dalam laporan tersebut. Bobot skor penilaian Indonesia sama dengan yang dikantongi Filipina.Sementara itu, Malaysia dikukuhkan sebagai negara yang memiliki keamanan siber terbaik di Asia Tenggara dengan skor 79,22 poin. Negeri Jiran ini juga mengisi peringkat ke-22 secara global. Kemudian Singapura berada di posisi kedua Asia Tenggara dengan skor keamanan siber 71,43 poin. Disusul Thailand yang meraih 64,94 poin. Sejumlah negara Asia Tenggara lainnya berada di bawah peringkat Indonesia, yakni Brunei Darussalam, Vietnam, Kamboja, Laos, dan Myanmar yang meraih skor kemaman siber kurang dari 50 poin. NCSI membuat penilaian ini berdasarkan sejumlah indikator, seperti aturan hukum negara terkait keamanan siber; ketersediaan lembaga pemerintah di bidang keamanan siber; kerja sama pemerintah terkait keamanan siber; serta bukti-bukti publik seperti situs resmi pemerintah atau program lain yang terkait.

Menanggapi tren ini, penelitian ini bertujuan untuk melakukan analisis mendalam terhadap perlindungan nasabah Bank Syariah Indonesia (BSI) terhadap potensi kebocoran data dalam pemanfaatan layanan digital banking. Penelitian ini mencakup pemahaman terhadap kebijakan keamanan yang diterapkan oleh BSI, respons terhadap serangan siber, dan kebijakan perlindungan data nasabah.

KAJIAN TEORITIS

1. **Perlindungan Konsumen**
   Perlindungan Konsumen adalah seperangkat tindakan yang dilakukan oleh pemerintah untuk melindungi konsumen dari praktik bisnis yang tidak adil dan merugikan. Dalam layanan keuangan digital, perlindungan konsumen diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.(Agus Iermansyah, Dhian Indah Astanti, 2021)
2. **Digital banking**
   Digital banking adalah layanan perbankan yang disediakan melalui platform digital seperti aplikasi seluler atau situs web. Layanan ini memungkinkan pengguna untuk melakukan transaksi perbankan seperti transfer uang, pembayaran tagihan, dan

pembukaan rekening tanpa harus mengunjungi cabang bank. Menurut penelitian yang dilakukan oleh Muhammad Nafik Hadi Ryandono, digital banking dapat meningkatkan efisiensi dan efektivitas layanan perbankan, serta memperluas akses ke layanan perbankan bagi masyarakat.(Ryandono, 2021)

PENELITIAN

Metode merujuk pada suatu pendekatan atau langkah-langkah yang harus diikuti dalam melakukan penelitian. Tujuan dari metode ini adalah untuk memberikan arahan, mencari, dan menemukan kebenaran ilmiah dengan rinci, serta dapat dijelaskan secara ilmiah tanpa menyimpang dari perumusan masalah yang diajukan. Penelitian ini mengadopsi jenis metodologi deskriptif kualitatif. Data yang digunakan terdiri dari literatur, berita, dan buku, dengan memperhatikan peraturan yang diberlakukan oleh regulator, yaitu Bank Indonesia dan Otoritas Jasa Keuangan. Metode ini dirancang untuk memastikan bahwa proses penelitian berlangsung sesuai dengan standar ilmiah dan memberikan hasil yang dapat dipertanggungjawabkan.(Mutiasari, 2020)

HASIL DAN PEMBAHASAN

Layanan Digital BSI

Digital banking mengacu pada digitalisasi produk, proses, dan aktivitas perbankan untuk memberikan layanan kepada nasabah melalui saluran online. Ini telah memainkan peran penting dalam era ekonomi digital dengan mengubah cara pelanggan berinteraksi dengan layanan perbankan. Munculnya perbankan digital telah menyebabkan peningkatan kenyamanan dan aksesibilitas bagi pelanggan, karena mereka sekarang dapat mengakses layanan perbankan 24/7 melalui ponsel, komputer, dan perangkat pintar.

Munculnya perbankan digital membuat nasabah, baik individu maupun perusahaan, menjadi lebih mudah dan nyaman dalam melakukan berbagai transaksi keuangan, bahkan membuka produk perbankan tanpa harus datang ke kantor cabang. Perkembangan perbankan digital juga mendorong bank tradisional untuk beradaptasi dengan cepat terhadap gelombang transformasi digital untuk mempertahankan basis pelanggan mereka. Secara keseluruhan, perbankan digital telah merevolusi cara pelanggan terlibat dengan layanan perbankan, memberi mereka fleksibilitas dan kenyamanan yang lebih besar dalam transaksi keuangan mereka.

Bank Syariah Indonesia (BSI) menawarkan layanan digital banking yang memungkinkan nasabah untuk mengakses layanan perbankan melalui perangkat digital seperti smartphone, tablet, atau komputer. Pelayanan digital berbasis digital pada BSI yaitu Pembiayaan BSI OTO, BSI Smart Agent, BSI Mobile, BSI Aisyah, Solusi Emas, BSI JadiBerkah id, BSI ATM CRM (Cash Recycle Machine), BSI Merchant Business, BSI API Platform, BSI Cardless Withdrawal, BSI Payment Point, BSI QRIS, Buka Rekening Online, BSI Net, Mitraguna Online, BSI Debt Card, BSI Debt OTP, Deposito Mobile, Griya Hasanah Online dan E-mas BSI Mobile.

Adapun transaksi digital BSI sampai Maret 2023 mencapai 143,59 juta transaksi atau mencakup 97% transaksi, sedangkan sisanya sebanyak 3% masih menggunakan layanan teller. Hal ini yang ikut serta mendorong peningkatan pengguna dari layanan digital perusahaan. jumlah user mobile banking meningkat dari waktu ke waktu, *user register* yang memiliki BSI Mobile mencapai 5,18 juta user, atau tumbuh *year on year* 37%.

Resiko Dan Ancaman Keamanan

Secara umum nasabah menghadapi berbagai risiko keamanan saat menggunakan layanan perbankan digital seperti risiko keamanan siber, phishing, malware, dan serangan denial of service (DoS). Risiko keamanan siber mencakup ancaman dari pihak yang tidak bertanggung jawab yang mencoba mengakses, merusak, atau mencuri data dan informasi penting dari sistem perbankan digital.

Layanan digital Bank Syariah Indonesia (BSI), mengalami gangguan atau eror selama beberapa hari pada 8 Mei 2023. Gangguan tersebut disebabkan oleh maintenance system dan indikasi adanya serangan siber. Nasabah mengeluhkan kesulitan mengakses layanan, seperti transaksi melalui aplikasi BSI Mobile, ATM, dan teller. Bank Syariah Indonesia (BSI) telah melakukan normalisasi layanan, termasuk pada jaringan ATM dan kantor cabang, serta bekerja sama dengan berbagai pihak terkait untuk memastikan keamanan sistem dan dana nasabah. Pihak BSI mengklaim layanan perbankan mulai beroperasi normal pada tanggal 11 mei 2023, namun masyarakat di media sosial justru berkata sebaliknya hingga sepekan layanan perbankan belum dapat digunakan. Tak lama kemudian muncullan isu peretasan data oleh hacker pada BSI.(Utami et al., 2023) Gangguan ini menunjukkan pentingnya peningkatan ketangguhan terhadap serangan siber dalam layanan digital perbankan. Transformasi digital perbankan juga harus disertai dengan kesiapan infrastruktur teknologi informasi, terutama dalam menjaga keandalan dan keamanan layanan digital perbankan.

Pada tanggal 16 Mei 2023, BSI mengonfirmasi bahwa data nasabah dan dana tetap aman meskipun terjadi gangguan layanan. Otoritas Jasa Keuangan (OJK) mendorong BSI untuk memastikan layanan tetap berjalan normal setelah insiden tersebut dan meminta semua lembaga keuangan di industri perbankan untuk memperkuat ketahanan digital mereka. Pada tanggal 18 Mei 2023, kelompok ransomware LockBit mengklaim telah mencuri 1,5 terabyte data dari BSI setelah negosiasi tebusan gagal. Ini menunjukkan bahwa BSI mengalami gangguan serius pada layanan digitalnya yang memengaruhi nasabah.

Di era digital yang semakin maju, kebocoran data menjadi tantangan yang serius di berbagai sektor, termasuk sektor perbankan. Kebocoran data pribadi sebenarnya bukanlah hal baru, namun merupakan masalah yang sangat serius dan memprihatinkan. Terungkapnya informasi pribadi nasabah seperti nomor rekening, informasi kartu kredit, data identitas, dan detail keuangan dapat memiliki dampak yang merugikan. Kebocoran semacam ini dapat terjadi karena serangan siber, pelanggaran keamanan internal atau kelalaian dalam pengelolaan data. Selain menimbulkan resiko pencurian identitas, penipuan, dan penyalahgunaan finansial, kebocoran data pribadi perbankan juga dapat mengancam kepercayaan nasabah terhadap institusi perbankan dan menyebabkan kerugian reputasi yang signifikan.

Perlindungan Hukum Terhadap Nasabah PT. Bank Syariah Indonesia Berdasarkan UU Perlindungan Konsumen

Perlindungan hukum terhadap nasabah PT. Bank Syariah Indonesia berdasarkan Undang-Undang Perlindungan Konsumen (UUPK) merupakan bagian integral dari hak asasi manusia untuk memenuhi kebutuhan hidupnya. Perlindungan konsumen adalah konsep yang harus diterapkan dalam kegiatan ekonomi, memastikan bahwa konsumen memperoleh barang dan jasa yang memenuhi standar kelayakan. Upaya pemerintah, termasuk pembentukan peraturan seperti UU No. 8 Tahun 1999, menetapkan perlindungan konsumen sebagai segala usaha untuk memberikan kepastian hukum.

Perlindungan hukum, pada dasarnya, adalah pemenuhan hak-hak konsumen yang seharusnya diberikan kepada mereka. Kewajiban melindungi konsumen tidak hanya terletak pada pemerintah, melainkan juga menjadi tanggung jawab pelaku usaha, termasuk bank seperti PT. Bank Syariah Indonesia. Perlindungan konsumen melibatkan berbagai aspek hukum, termasuk hukum perdata, administrasi, dan pidana, serta tidak hanya terbatas pada ganti rugi atau sanksi kepada pelaku usaha.

Dalam perlindungan terhadap nasabah, ada dua pendekatan: perlindungan tidak langsung terhadap resiko kerugian yang mungkin timbul dari kebijaksanaan atau kegiatan usaha bank, dan perlindungan langsung terhadap resiko kerugian yang muncul dari kegiatan usaha bank. Nasabah PT. Bank Syariah Indonesia, sebagai konsumen akhir, dilindungi oleh UUPK, dan hubungan antara nasabah dan bank diatur oleh UU No. 8 Tahun 1999.(Marcelliana et al., 2023)

Kasus pencurian data yang terjadi pada nasabah PT. Bank Syariah Indonesia menunjukkan pelanggaran hak-hak konsumen berdasarkan UUPK. Pasal 4 UUPK memberikan dasar hukum bagi nasabah yang dirugikan untuk mendapatkan kompensasi, ganti rugi, dan/atau penggantian terhadap jasa yang tidak sesuai dengan janji yang diberikan. Pelanggaran ini termasuk ancaman terhadap data nasabah akibat serangan siber.

Kewajiban pelaku usaha, dalam hal ini PT. Bank Syariah Indonesia, termaktub dalam Pasal 7 huruf D dan G UUPK. Bank diwajibkan menjamin mutu jasa yang berdasarkan standar mutu yang berlaku dan memberikan ganti rugi sesuai dengan kerugian yang dialami oleh nasabah. Standardisasi keamanan, terutama dalam produk perbankan, menjadi kewajiban yang harus dilaksanakan dengan baik oleh bank.

Protokol Keamanan yang Diterapkan oleh BSI

Bank Syariah Indonesia (BSI) telah mengimplementasikan berbagai tindakan keamanan untuk melindungi nasabahnya. Untuk mengatasi serangan ransomware, perusahaan yang jadi korban mesti menghubungi penegak hukum, lembaga yang menangani darurat serangan siber, atau pun perusahaan keamanan siber. Beberapa teknologi keamanan yang digunakan oleh BSI antara lain enkripsi data, otentikasi dua faktor, dan sistem keamanan lainnya. BSI telah mengalokasikan belanja modal sebesar Rp 580 miliar untuk memperkuat digitalisasi dan keamanan data. Hal ini dilakukan sebagai respons terhadap gangguan layanan dan isu kebocoran data yang terjadi beberapa waktu lalu. BSI juga menekankan bahwa anggaran tersebut akan digunakan untuk pengamanan data dan layanan perbankan. BSI melakukan langkah preventif penguatan sistem keamanan teknologi informasi terhadap potensi gangguan data dengan peningkatan proteksi dan ketahanan sistem. BSI berkoordinasi dengan pihak terkait, seperti Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), dan Bank Indonesia (BI).

Pengelolaan Kejadian Keamanan (Security Incident Management):

Perkembangan digitalisasi di sektor perbankan meningkatkan timbulnya risiko terhadap keamanan siber bagi Bank. Maraknya serangan siber telah mendorong kebutuhan untuk meningkatkan ketahanan siber (cyber resilience) melalui penguatan keamanan siber (cyber security). Penguatan keamanan siber telah mengarah kepada berbagai insiatif di berbagai sektor industri tak terkecuali sektor perbankan untuk mengatasi risiko siber (cyber risk) oleh para regulator di berbagai negara. (OJK, 2020)

Terlebih lagi, sektor keuangan termasuk perbankan merupakan sektor yang menjadi target serangan siber paling tinggi baik secara global maupun di Indonesia. Berdasarkan catatan Bank for International Settlements (BIS), regulator perbankan di beberapa negara

telah memiliki kebijakan khusus terkait keamanan siber. Beberapa best practices di berbagai negara yang bertujuan untuk meningkatkan keamanan siber antara lain mencakup kebijakan terkait pengelolaan keamanan siber, kewajiban penilaian risiko siber, kewajiban pengujian kerentanan teknologi informasi Bank, penilaian tingkat maturitas siber, dan pelaksanaan pengujian keamanan siber Bank.(OJK, 2020)

Menurut Dr. Pratama Persadha, Kepala Lembaga Riset Keamanan Siber CISSReC, sistem pertahanan siber di bank-bank Indonesia dinilai tidak cukup kuat, dan hal ini tampaknya menjadi masalah yang lebih luas dengan beberapa bank sebelumnya mengalami serangan siber, termasuk Bank Indonesia pada awal 2022.

Penting bagi Bank Syariah Indonesia dan bank-bank lainnya di Indonesia untuk memperkuat sistem pertahanan digital mereka mengingat sektor keuangan, khususnya perbankan, menjadi target serangan siber paling tinggi baik secara global maupun di Indonesia. Langkah-langkah yang perlu dipertimbangkan termasuk penerapan kebijakan terkait pengelolaan keamanan siber, kewajiban penilaian risiko siber, pengujian kerentanan teknologi informasi, penilaian tingkat maturitas siber, dan pelaksanaan pengujian keamanan siber, sesuai dengan best practices yang telah terbukti di berbagai negara.

Meskipun peningkatan keamanan jaringan dan sistem melalui penerapan firewall, enkripsi data, dan pemantauan aktif dapat membantu mencegah serangan siber, tidak ada jaminan bahwa suatu sistem akan sepenuhnya aman dari serangan ransomware. Oleh karena itu, penting untuk mengimplementasikan mitigasi yang benar dan melakukan persiapan yang baik. Best practices yang telah terbukti, seperti yang telah diimplementasikan di berbagai negara, seharusnya juga dipertimbangkan untuk diadopsi oleh bank syariah Indonesia guna memitigasi potensi ancaman dan kerentanan siber yang dapat mengancam keamanan digital mereka.

Bentuk Pertanggungjawaban PT. Bank Syariah Indonesia Terhadap Nasabah Berdasarkan Undang-Undang

PT. Bank Syariah Indonesia memiliki tanggung jawab terhadap kebocoran data nasabah berdasarkan prinsip-prinsip pertanggungjawaban dalam Undang-Undang Perlindungan Konsumen (UUPK). Pertanggungjawaban ini tidak terlepas dari prinsip tanggung jawab perdata yang mencakup beberapa aspek.

a. Prinsip tanggung jawab berdasarkan unsur kesalahan, mengindikasikan bahwa seseorang dapat dimintai pertanggungjawabannya jika terbukti melakukan kesalahan. Hal ini sesuai dengan Pasal 1365 KUHPerdata yang mengharuskan penggantian kerugian akibat perbuatan melanggar hukum.
b. Prinsip praduga untuk selalu bertanggung jawab menempatkan beban pembuktian pada tergugat, di mana tergugat dianggap bertanggungjawab sampai dapat membuktikan tidak bersalah. Prinsip ini mendorong tanggung jawab terhadap setiap kerugian yang bersalah.
c. Prinsip praduga untuk tidak selalu bertanggung jawab terbatas pada transaksi konsumen dengan pembatasan yang bisa dibenarkan secara common sense.
d. Prinsip tanggung jawab mutlak atau strict liability menetapkan tanggung jawab tanpa mempertimbangkan unsur kesalahan, meskipun ada pengecualian seperti force majeure.
e. Prinsip tanggung jawab dengan pembatasan mengacu pada pembatasan tanggung jawab yang seharusnya tidak merugikan konsumen dan harus sesuai dengan peraturan perundang-undangan yang jelas.

Dalam UUPK, prinsip pertanggungjawaban mutlak mengarahkan bahwa PT. Bank Syariah Indonesia harus bertanggung jawab atas kebocoran data nasabah tanpa perlu pembuktian unsur kesalahan. UUPK juga mengatur bentuk ganti rugi terhadap perbuatan melawan hukum, seperti ganti rugi nominal, ganti rugi kompensasi, dan ganti rugi penghukuman.(Marcelliana et al., 2023) Sejalan dengan hal tersebut, Dalam Undang-Undang Nomor 21 Tahun 2008 Pasal 47 ayat (1) tentang perbankan syariah dalam UU tersebut menyatakan bahwa bank syariah wajib menjamin kerahasiaan data dan informasi nasabah. Jika terjadi kebocoran data nasabah, maka bank syariah harus bertanggung jawab atas kerugian yang timbul, kecuali dapat membuktikan bahwa kebocoran tersebut bukan karena kesalahan bank syariah. Selain itu, Pasal 48 ayat (1) UU tersebut mengatur bahwa bank syariah wajib memberikan ganti rugi atas kerugian yang diderita nasabah akibat perbuatan melawan hukum yang dilakukan oleh bank syariah atau pegawainya. Ganti rugi tersebut dapat berupa ganti rugi nominal, ganti rugi kompensasi, dan ganti rugi penghukuman.

Dalam kasus kebocoran data nasabah BSI yang diduga dilakukan oleh hacker, prinsip-prinsip tersebut menunjukkan bahwa BSI harus memberikan ganti rugi kompensasi kepada nasabah yang terdampak. Kasus ini berdampak kerugian pada nasabah, sehingga pihak bank wajib mengganti kerugian sesuai dengan aturan yang berlaku. Nasabah berhak untuk menuntut ganti rugi melalui jalur hukum yang sesuai dengan peraturan yang berlaku, dengan beban pembuktian terletak pada pihak nasabah yang bermasalah.

Dengan pertumbuhan ekonomi digital yang pesat, perlindungan nasabah dalam pemanfaatan layanan digital banking menjadi esensial, dan implementasi perlindungan hukum serta kebijakan keamanan yang efektif akan menjadi landasan penting bagi keberlanjutan dan kepercayaan nasabah dalam era ekonomi digital. Oleh sebab itu guna mecapai keberhasilan dalam era ekonomi digital bank syariah wajib untuk lebih ketat dalam melindung data dari nasabah atau konsumenya.

KESIMPULAN DAN SARAN

Penelitian ini bertujuan untuk menganalisis perlindungan nasabah Bank Syariah Indonesia (BSI) terhadap potensi kebocoran data dalam pemanfaatan layanan digital banking di era ekonomi digital yang berkembang pesat. Transformasi digital perbankan, khususnya di Indonesia, terlihat dari peningkatan transaksi digital banking yang mencapai Rp5,1 kuadriliun pada bulan Agustus 2023. Meskipun memberikan kemudahan dan efisiensi, penggunaan layanan digital banking juga membawa risiko keamanan yang signifikan, termasuk ancaman siber. Insiden gangguan layanan pada Mei 2023, disebabkan oleh maintenance system dan serangan siber, menunjukkan pentingnya peningkatan ketangguhan terhadap serangan siber dalam layanan digital perbankan.

Keamanan siber di sektor perbankan menjadi fokus utama mengingat peningkatan jumlah serangan siber. Indonesia masuk dalam lima besar negara dengan keamanan siber terbaik di ASEAN menurut laporan National Cyber Security Index (NCSI). Namun, masih ada tantangan, dan penelitian ini menganalisis perlindungan nasabah BSI melalui pemahaman terhadap kebijakan keamanan, respons terhadap serangan siber, dan kebijakan perlindungan data nasabah. Perlindungan hukum terhadap nasabah BSI berdasarkan Undang-Undang Perlindungan Konsumen (UUPK) menjadi hal krusial. Prinsip-prinsip pertanggungjawaban, baik yang berkaitan dengan kesalahan, praduga tanggung jawab, maupun tanggung jawab mutlak, menjadi dasar dalam menilai kewajiban BSI terhadap nasabah akibat kebocoran data. Bank Syariah Indonesia harus memperkuat sistem pertahanan siber, mengimplementasikan teknologi keamanan seperti

enkripsi data, otentikasi dua faktor, dan bekerja sama dengan lembaga terkait seperti Badan Siber dan Sandi Negara (BSSN), Otoritas Jasa Keuangan (OJK), dan Bank Indonesia (BI).

penelitian ini memberikan pemahaman terhadap protokol keamanan dan pengelolaan kejadian keamanan yang dapat diterapkan oleh BSI. Dengan pertumbuhan ekonomi digital yang pesat, perlindungan nasabah dalam pemanfaatan layanan digital banking menjadi esensial, dan implementasi perlindungan hukum serta kebijakan keamanan yang efektif akan menjadi landasan penting bagi keberlanjutan dan kepercayaan nasabah dalam era ekonomi digital.

DAFTAR REFERENSI

Agus Iermansyah, Dhian Indah Astanti, dan B. R. H. (2021). PERLINDUNGAN HUKUM BAGI KONSUMEN DALAM JASA LAYANAN KEUANGAN (DIGITAL FINANCIAL TECHNOLOGY). *Hukum Dan Peradilan*, *10*(2), 1–14.

Ardianto, P. (2023). *kuartal I 2023, Pengguna BSI Mobile Tembus 5,18 Juta*. BeritaSatu.Com. https://www.bing.com/search?q=jurnal+jumlah+pengguna+digital+banking+bsi&qs=n&form=QBRE&sp=-1&lq=0&pq=jurnal+jumlah+pengguna+digital+banking+bsi&sc=10-42&sk=&cvid=BAEDFD4024864DE69205A24B3F59F6BE&ghsh=0&ghacc=0&ghpl=&showconv=1

Marcelliana, V., Zahra, S. M., Adzani, N. N., Massaid, H. N., Badriyyah, N., Benita, R., Sukarto, M., Fitriani, C. N., & Bayhaqi, T. A. R. (2023). PENERAPAN PERLINDUNGAN KONSUMEN TERHADAP NASABAH PT. BANK SYARIAH INDONESIA DALAM KASUS KEBOCORAN DATA NASABAH. *Publikasi Ilmu Hukum*, *1*(2), 180–194. https://doi.org/https://doi.org/10.59581/deposisi.v1i2.562

Mutiasari, A. I. (2020). PERKEMBANGAN INDUSTRI PERBANKAN DI ERA DIGITAL. *EKONOMI BISNIS DAN KEWIRAUSAHAAN*, *IX*(2), 33.

OJK. (2020). Cetak Biru Transformasi Digital Perbankan. *Ojk*, *13*(April), 1–54.

Rahmah, Y. N. (2018). PENGARUH PENGGUNAAN INTERNET BANKING DAN PERLINDUNGAN NASABAH PENGGUNA FASILITAS INTERNET BANKING TERHADAP CYBER CRIME DI DAERAH 'ISTIMEWA YOGYAKARTA. *Ekonomi Dan Bisnis*, *1*(2), 580.

Rizki, M. J. (2022). *Risiko dan Langkah Mitigasi Serangan Siber Sektor Perbankan Digital*. Hukum Online. https://www.hukumonline.com/berita/a/risiko-dan-langkah-mitigasi-serangan-siber-sektor-perbankan-digital-lt62846d0e25570/

Ryandono, M. N. H. (2021). Pengaruh Digital Banking Terhadap Efisiensi dan Efektivitas Layanan Perbankan. *Ilmiah Mahasiswa FEB*, *10*(2), 1–12.

Utami, N., Subagiyo, R., & Asiyah, B. N. (2023). Reputational Risk Management Strategy At Indonesian Sharia Bank and Muamalat Indonesian Bank. *Balance: Journal of Islamic Accounting*, *4*(1), 19–39. https://doi.org/10.21274/balance.v4i1.7726